Comparative Analysis and Application of Common Authentication and Accounting Technology in the Modern Network

JunJie Zhou, Yaowei Yan, Lei Wang,Yiming Guo

Wenhua College, Huazhong U. of Sci. & Tech. Wuhan, China

zjj0718@126.com; yanyaw@126.com

Abstract

Through technical analysis and comparison of authentication modes and architecture of commonly used network accounting technology such as PPPoE + Radius, DHCP + WEB + Radius, 802.1X + Radius, Kerberos and SSO, it is revealed in this paper that Kerberos as a new mode is suitable for the application of Web network system identity Authentication; while in many cases SSO can access all the mutually trusted application system by means of a single login; and in modern broadband Ethernet access, optimized IEEE 802.1x protocol + Radius server authentication mode is recommended, which can solve the bottleneck problem of the traditional authentication methods such as PPPoE and Web / Portal.

Keywords

PPPoE; Web Portal; 802.1X + Radius; Kerberos; SSO; Authentication and Accounting

PPPoE + Radius Mode

Briefing and Principles

Came out in late 1998, Point to Point Protocol over Ethernet (PPP over Ethernet, PPPoE) technology was developed jointly based on IETF RFC by Redback Networks company, client software developer Router Ware company and the subsidiary of Worldcom – UUNET Technologies company. With the main purpose of the combination of the most economical LAN technology, extendibility and management control functions of Ethernet and Point to Point Protocol together, it allows service providers to offer more user-friendly support in multi-user broadband access services through digital subscriber line, cable modem or wireless connections, etc.

The establishment of PPPoE requires two stages, namely the Discovery stage and PPP Session stage. When a host wants to initiate a PPPoE session, the Discovery stage must be completed at first to determine the terminal Ethernet MAC address, and then a PPPoE session number (Session-ID) is established. At the time of PPP protocol defining a relationship between two terminal devices, the Discovery stage is a client – server relationship. In the process of the Discovery Stage, the host (client) searches and finds a network device (server). In the network topology, the host can communicate with more than one network devices. Though the host in the Discovery stage can find all the network devices but he can only choose one. After the successful completion of the Discovery stage, the host and network equipment will have all the information to establish the PPPoE. Discovery stage will exist until the PPPoE session is built, after which, host and network devices must provide resources for the virtual interface of the Session stage.

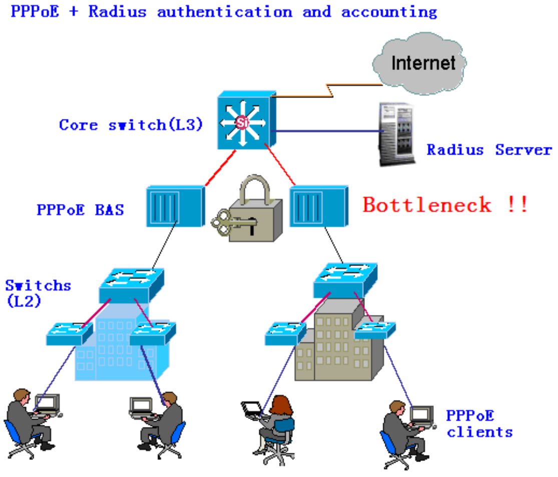


FIG.1 THE PPPOE + RADIUS AUTHENTICATION AND ACCOUNTING MODE

The Advantages and Disadvantages of PPPoE

Advantages:

- An extension of traditional PSTN narrowband access technique on the Ethernet access technology.

- Consistent with the original narrowband network access authentication system.
- End users are relatively easy to accept.

Disadvantages:

- PPP protocol with significant difference from Ethernet technique, needs to be encapsulated into Ethernet frame again, resulting in the low efficiency.
- PPPoE generates a lot of broadcast traffic in Discovery stage, which has great impact on network performance.
- The multicast business has many difficulties, while video business is mostly based on multicast.
- Requirement for operators to provide the client terminal software; and the maintenance workload is excessive.
- PPPoE authentication generally needs external BAS(Broadband Access Server, the core equipment certification system). After the authentication, the business data flow must also get through the BAS equipment, which is easy to cause the single point bottleneck and fault, and usually the equipment is very expensive.

DHCP + Web + Radius Mode

Briefing and Principles

Web authentication, which has already been the authentication mode of operator network platform, implements authentication through the Web page by judging whether users are granted with the right to access it.

The main process of Web authentication is listed below.

When the user’s computer first starts, system program makes the DHCP-relay by BAS according to the configuration, and then the DHCP Server is asked for IP address;

BAS structures table information (based on the port number and IP) for the corresponding user and adds user ACL （Access Control List） service strategy (so that users can only access the portal server and some internal servers, or individual external servers such as DNS);

The portal server provides the authentication page for users, in this page the user inputs account and password and clicks the button of login, or directly clicks the button without inputting. The login button starts a program on the portal server, which sends user information (IP address, account and password) to network center equipment BAS;

BAS uses IP address to get user layer 2 address and physical ports (such as VLAN ID, ADSL, PVC ID, or PPP session). By means of such information, BAS checks the legitimacy of the user. If the user inputs the account, it is considered as card user and authenticated by radius server with the account and password. If the user does not input the account, it is regarded as fixed user, and then the network equipment looks up the user table for user's account and password by VLAN ID or PVC ID before it is authenticated by Radius Server;

Radius Server returns the authentication result to the BAS;

After authentication, BAS modifies the user's ACL; then users can access the Internet or external specific network services;

Before a user cuts off the network, it connects to the portal server and charging system can be stopped by clicking the button of logout, which deletes a user's ACL and forwarding information as well as restricts user's access to the external network.

In this process, attention must be paid to cases of users cutting off network abnormally, such as user host crash, network dropping, or direct power off.

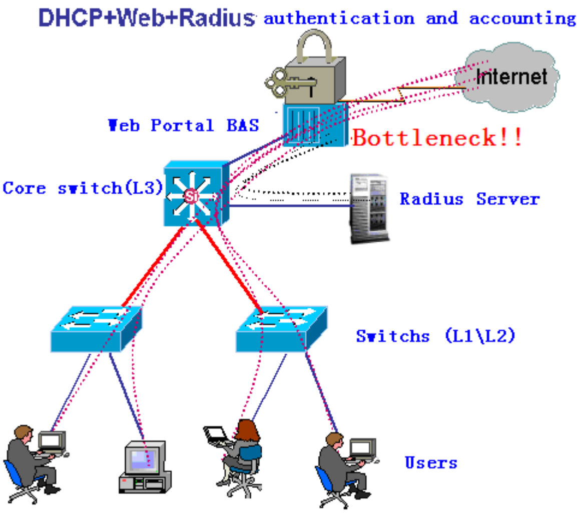


FIG. 2 DHCP + WEB + RADIUS AUTHENTICATION AND ACCOUNTING MODE

The Advantages and Disadvantages of DHCP + Web

Advantages:

- With no need for special client software. Low maintenance cost on workload.

- The offer of business authentications such as portal.
- Disadvantages:
- Web hosts in the layer 7 protocol, which needs higher devices and more cost on network construction.
- Degraded standardization and openness. The use of private communication protocol between the authentication equipment and Web.
- Poor connectivity with user. Difficulty in detection of whether the user is offline as well as in the achievement of time-based accounting.
- Ease of use is not enough. When the user accesses the network, by means of irregardless Telnet, FTP, or other business, a browser is a must to be employed for Web authentication.
- The allocation of IP address is previous to user authentication. If the user is not the dial-up user, it causes address waste. In addition, it is not convenient for multi-ISP support.
- Business flow and control flow cannot be distinguished before and after authentication, thus a lot of CPU resources are consumed.

802.1X + Radius Mode

What is IEEE 802.1X Protocol

IEEE 802.1X is a port-based network access control protocol.

The architecture of IEEE 802.1X protocol includes three important parts: Supplicant System, Authenticator System and Authentication Server System.

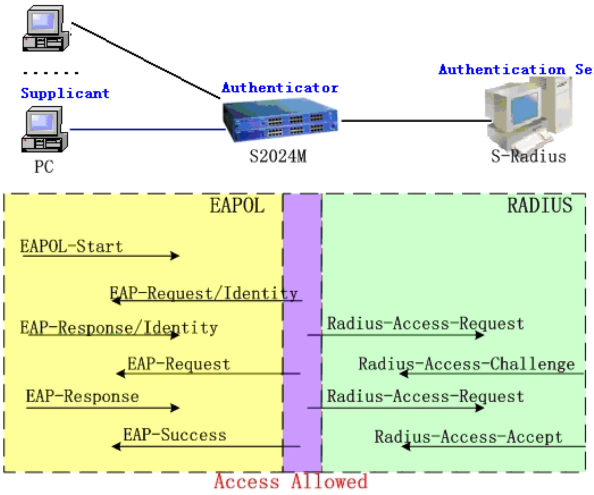


FIG. 3 802.1X + RADIUS AUTHENTICATION MODE

The IEEE 802.1X Protocol Technical Characteristics

1) The Implementation Simpleness

IEEE 802.1X protocol , a layer 2 protocol , excludes layer 3, so it is less demanding on the overall performance of the device, resulting in considerable decrease of network construction cost.

2) The Authentication and Business Separation

IEEE 802.1X authentication architecture adopts "controlled port" and "uncontrollable port" logic functions, which achieves the separation of business and authentication. After the user is authenticated, business and authentication flow are detached. There are no special requirements on the following packet processing. The business can be very flexible. Especially, the method holds great advantage in the implementation of the business of broadband multicast, and no business is limited by the authentication mode.

3) The Comparison with Other Modes

IEEE 802.1X protocol is derived from IEEE 802.11 wireless Ethernet (EAPOW). However, its introduction into the Ethernet has solved the problems brought by traditional PPPoE and Web / Portal authentication, eliminated network bottlenecks, reduced encapsulation overhead of the network, and abated the cost of network construction.

Advantages of IEEE 802.1X

Concision and efficiency: pure Ethernet technology kernel; t connectionless characteristic of IP network; removal of redundancy in expensive multi-service gateway device; elimination of network authentication accounting bottleneck and single point of failure; easy to support multi-service.

Ease of implementation: it can be implemented on ordinary L2, L3, IP, DSLAM; and the network comprehensive cost is low.

Security and reliability: the acquisition of user authentication on layer 2 network; combined with MAC, port, account and password, etc., the binding technology with high security .

Industry standards: IEEE standard, built-in support by Microsoft operating system.

Ease of operation: completion of separation of control flow and business flow; easiness in implementation of multi-service operation; an achievable carrier-grade network by means of small amount of transformation from the single fee system such as the traditional monthly subscription network.

802.1X + Radius Security Authentication and Accounting System Solutions

According to the need of user, the SAM system of RG company can be used to build a network of security authentication and accounting system in student dormitory; in which the core technology is 802.1x + Radius constitution. In addition, the whole authentication and accounting system consists of several parts of the safety switches (such as S2126G), S-Radius server, DHCP server and portal server. The specific implementation mode is shown below.

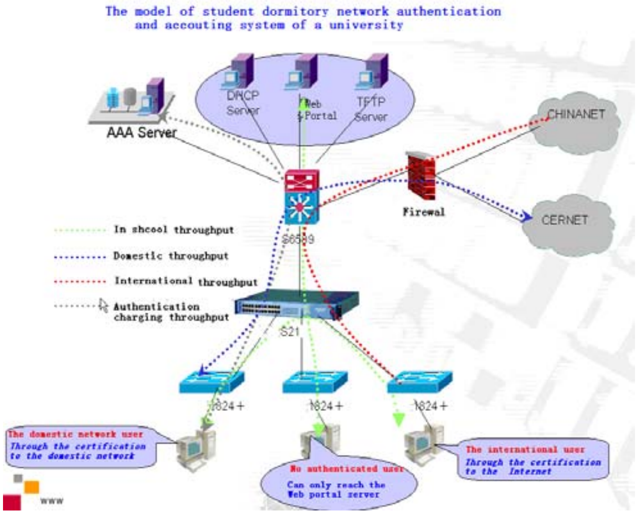

The model of student dormitory network authentication and accouting system of a university
AAA Server
DHCP Server
Web Portal
TFTP Server
CHINANET
Firewal
CERNET
S6509
In shcool throughput
Domestic throughput
International throughput
Authentication charging throughput
S21
1824+
1824+
1824+
The domestic network user
Through the certification to the domestic network
No authenticated user
Can only reach the Web portal server
The international user
Through the certification to the Internet
www

FIG. 4 802.1X + RADIUS SECURITY AUTHENTICATION AND ACCOUNTING SYSTEM MODE

Kerberos Network Authentication

What is Kerberos Protocol

Kerberos is a network authentication protocol, whose design objective is to provide strong authentication for client/server applications through the key system. Implementation of the certification process, independent of the authentication of the host operating system, and exclusive from the need of trust based on host addressas well as the physical security of all the hosts on the network, assumes that the data packets transmitted on the network can be freely read, modified and inserted with data. In the above cases, as a trusted third party, the Kerberos authentication service performs certification services by means of traditional cryptographic techniques, for example, shared key.

The Kerberos Authentication Process

First of all, the client sends a request to the authentication server (AS) for a server certificate. The response of the AS contains the certificate encrypted by the client key. The certificate contains: 1) the server "ticket"; 2) a temporary encryption key (also known as the session key). The client transmits the ticket (including the client identity encrypted by the server key, and a copy of the session key) to the server. Session key (currently be shared between the client and the server) i utilized for authentication of the client or the authentication server, can be used to provide encryption services for the subsequent communication, or by exchanging the independent sub-session key for the two communicating parties to provide further communication encryption services.

Two Parts of the Kerberos Protocol

1. The client sends its own identity information to key distribution center KDC getting TGT (Ticket-Granting Ticket) from the Ticket Granting Service, and replying the TGT encrypted by key between Client and KDC before the starting of the protocol.

At this time only true client can use the encryption key between itself and KDC to decrypt the encrypted TGT.

This process avoids unsafe way: client sending the password directly to the KDC.

2. The client uses the TGT obtained before to request the ticket of other services from KDC.

The Defects of Kerberos

1. Single point of failure: it requires a sustained response to the central server. Before the end of the Kerberos service, no one can connect to the server. This defect can be compensated by using composite Kerberos server and the defect certification mechanism.

2. Kerberos request hosts participating in communication to be clock-synchronized. The ticket is of timeliness; therefore, if the host is not synchronical with the Kerberos server, authentication will fail. The default configuration requires that clock time do not differ with more than 10 minutes. In practice, usually the network time protocol daemon is used to keep the hosts synchronization.

3. Management protocol is not standardized; and there are some differences in the server implementation tools.

4. All user keys are stored on a central server; acts that endanger the security of the server will endanger the entire keys.

5. dangerous client will hazard the user password.

The Single Sign-On Authentication Technology Based on Digital Certificate

SSO Profile

SSO . based on digital certificate single sign-on technique, assembles the information resources and the protection system station as organic whole, communicates with authentication server of protection system by installing access control agent middleware in various information resource ends, and shares advantages in security bulwark and information services provided by the system.

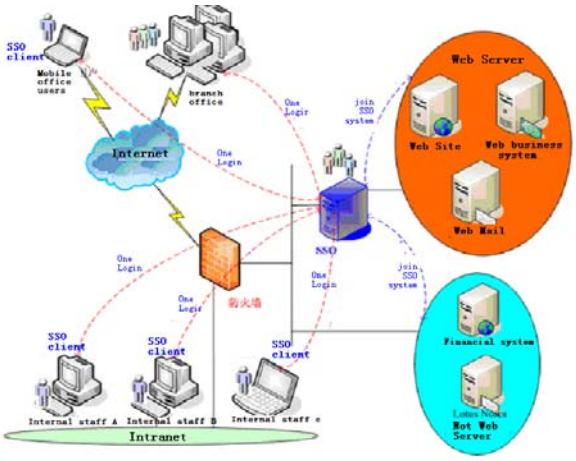


FIG. 5 THE SSO AUTHENTICATION TECHNOLOGY SYSTEM INTERACTION

SSO Principle

Its principles are as follows:

1. Configure an access agent for each information resource, and allocate different digital certificate to different agent, which is used to guarantee the secure communication between itself and system service.

2. When the user login the center, the identity of the user is confirmed according to the digital certificate provided by the user.

3. When a specific information resource is assessable, system service sends encrypted user identity information by the agent-corresponding digital certificate in the form of digital envelope to the related information resource server.

4. After the information resource server receives the digital envelope, it performs decryption and validation via access agent to get the user identity, on which it authenticates the internal permission.

SSO Application Advantages

1. Single sign-on: By a simply log in once, the user can access multiple applications of the background through a single sign on system, and the second landing doesn't need re-enter the user name and the password.

2. C/S single sign on solution: there is no need in the modification of any existing application system service and client to implement the C/S single sign on system.

3. Self installation: by simple configuration, it can be utilized without modifying any of the existing B/S or C/S application systems.

TABLE 1 TECHNICAL COMPARISON OF THE VARIOUS AUTHENTICATION MODES

Modes	PPPoE	WEB Portal	802.1X	Kerberos	SSO
Standard level	RFC 2516	Private	IEEE Standard	RFC1510/4120	No
Encapsulation Overhead	Relatively hign	Low	No	High	Relatively hign
Access Control	User	VLAN-MAC-IP	User	Centralized user / system default	User/system control/ Agent
IP Address Allocation	After authentication	Before authentication	After authentication	May not allocate	Not need to allocate
Multicast Support	Poor	Good	Good	Support	Support
VLAN Demand	No	Much	No	No	No
Client Software	Need	Browser	Need	OS build-in	Need/Browser
Device Support	Public protocol	Manufacturer private	Public protocol	Public protocol	Public and compatible
User Connectivity	Good	Poor	Good	Relatively good	Good / With DB ticket user can shares resources
Device Performance Requirements	Relatively High (BAS)	High (Whole course VLAN)	Low	High	Relatively High (Multi-system)

4. Application flexibility: Embedded dynamic domain name system (for example: gnHost) can be implemented independently, or combined with other products.

5. Role-based access control: access control functions are based on the user's role and URL.

6. A comprehensive audit of the log: a log of the user query is recorded accurately; and statistics and analysis on the log are based on the dates, addresses, users, resources and other information

7. Cluster: Via clustering capabilities, dynamic load balance between multiple servers can be achieved.

8. Transmission encryption: Support for a variety of symmetric and asymmetric encryption algorithmsto prevent user information from being stolen and tampered during transmission.

9. Scalability: good compatibility with subsequent expansion and extension of the business system.

Conclusion

It is well known that in the modern network system, usually a variety of components such as user terminals, NAS, Radius Server and database are used to build authentication and accounting system, which aims to achieve network security access control, billing, operations management, and provide a AAA (Authentication, Authorization, and Accounting) network security services framework. In many cases, the AAA needs to manage the security protocols, for instance, RADIUS, TACACS, and Kerberos, etc. This paper researches the secure authentication and accounting technologies in modern networkby means of analysis on protocols comparatively, including PPPoE, WEB Portal, Radius, 802.1X, Kerberos and SSO, and meantime, it summarizes their features as followed in Table I, for better service applied to network system of the cloud era.

REFERENCES

A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1X Standard," http://citeseer.nj.nec.com/, 2002.

G. Xiao, Z. Zhang and F. Wang, Digital certificate based single-point sign-on technology research and application Enterprise Technology Development, 2009.

L. Zhang, "Discussion about Kerberos Authentication and its Application in Middleware Tuxedo," Science Mosaic, No. 3, pp. 2, 99-100, 2008.

L. Zhang, The 802.1X-based campus network authenticationAcademic Journal of Guangdong College of Pharmacy, No. 6, 2004.

Q. Bi, "PPPOE Broadband Access Technonogy and Ordinary Failure Analyze, " China Cable Television, No. 8, 2004.

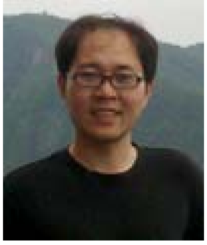
X. Xie, Computer Network (fifth edition). Beijing: publishing house of electronics industry, 2008.

Y. Bian, "QinQ solve PPPoE broadcast before authentication, Computer and Information Technology, 2008.

Junjie Zhou, 1979.07, male, Wenhua College, Huazhong University of Science and Technology. He possesses the "dual professional titles type "teacher(lecturer, engineers), and in 2004, he gained computer application technology professional master's degree. His main research area include the (wireless) network systems integration and engineering design, information system development etc.

Since 2003, the author successively to work in Hunan Agricultural Broadcasting and Television University, Huazhong University of Science and Technology Industry Group Corporation, Huazhong University of Science and Technology Wenhua College. Currently, he serves as the laboratory director of Computer Science and Technology. As for teaching work, he lectures the courses of "Computer network and applications", " Network security technology" etc. The author has written three textbooks " network systems integration and engineering design case tutorial ";along with two experimental handouts; and 7 EI / ISTP core journals / international conference papers;in addition, he is responsible for two transverse research projects and participate in many education reform issues, and he has awarded the provincial science and technology achievement appraisal, several college faculty awards.

With nearly 10-year advanced enterprise and the college experienced practitioners, the author has hold a concurrent post of the member of CCF(the China Computer Federation), ACM and IEEE-CS, the China National Institute for Occupational Skill Testing Center (Hubei District) network technology evaluation staff, the Ministry of Information Industry Computer Information System Integration certification project manager, AMD64-bit server certification engineers, Star-network Ruijie company the RCSE network engineers, NIIT (Indian Institute of Information Technology) GNIIT and NetPlus certified engineers.



Yaowei Yan, 1980. 11, male, lecturer of Wenhua College, Huazhong University of Science and Technology. The author has written two textbooks: "Computer network technology and applications" and "Web design and production tutorials", and published 5 EI international conference papers and a core journal paper.